Sible Hedingham Parish Council Data Security Policy

Introduction

Sible Hedingham Parish Council recognises the importance of meeting our data security obligations and is committed to being transparent about how it collects and uses data. This policy sets out the parish council's commitment to data security, and your rights and obligations in relation to personal data in line with the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA)

The Lawful Basis of Processing

- The data subject has personally **consented** to the processing of personal data e.g. signing up for a newsletter or involvement in a project or activity.
- The processing is necessary in accordance with a **contract** of employment between the data controller and the data subject.
- The processing is required in pursuance of a **legal obligation** – data needs to be processed by law.
- **Vital Interest**; when necessary for an individual's safety or protection of life.
- The processing is necessary for carrying out a **task in the public interest**; for example correspondence.
- When no other lawful basis applies, **legitimate interest** can be used but must be risk assessed.

Personal Data

Personal data as defined in GDPR Article 4, is information held in recorded form, both electronically and in writing, from which a living person can be identified directly or indirectly on its own or when combined with other details.
Article 5 (1) requires that personal data be processed "fairly, lawfully and in a transparent manner". Personal data will not be considered to be processed fairly unless certain conditions are met. A data subject is also entitled to know the identity of the data controller and why information is, or is to be, processed.

NB: The UK Data Protection Authority is the Information Commissioners Office (ICO) and ICO guidance should be followed at all times ico.org.uk

Purpose of the Data Security Policy

The purpose of this policy is to ensure Councillors, staff and other authorised users handle data the same safe and lawful way.

1. Data Security

1.1 A local council routinely holds and uses information about individuals in the performance of its statutory functions, powers and contractual obligations. Risks arise when data is moved outside secure council systems by the use of personal email accounts, use of own devices and information storage media. A clear Data Security policy sets out the rules for how information is stored, shared and protected. **This policy links with the IT and Email policy; for more detailed guidance please read the IT and Email policy siblehedingham-pc.gov.uk/policies-and-procedures/**

- **Equipment 2.1 – 2.9**
- **Use of own devices 3.1 – 3.6**

Responsibility

The responsibility for data security lies with the Clerk of the Parish Council as Data Controller. The Data Protection Officer is Kim Cole at Braintree District Council.

1.2 Passwords and Multi-Factor Authentication

All user accounts must be protected by strong, secure passwords. In addition to strong passwords, Multi-Factor Authentication (MFA) should be enabled wherever possible. MFA is a security process that requires users to verify their identity using two or more independent methods – for example, entering a password (something you know) and confirming a code sent to your mobile device (something you have). This significantly reduces the risk of unauthorised access to systems and sensitive data. NALC recommends implementing MFA as a best practice to enhance information security and support compliance with data protection obligations under the UK GDPR and the Data Protection Act 2018. This significantly reduces the risk of unauthorised access to systems and personal data and further strengthens account security. Al accounts no longer in use should also be removed. **For more detailed guidance please read the IT and Email policy**
siblehedingham-pc.gov.uk/policies-and-procedures/

- **Password and Authentication policy 5.1**
- **Access to passwords 6.1**
- **Password storage and management 6.2**
- **Password change requirements 6.3**
- **Password access control and logging 6.4**
- **Responsibility 6.5**

1.3 Emails

All Councillors and Clerks have .gov.uk email addresses and only these can be used for parish council business. Email messages sent on the council's account are for council use only; personal use is not permitted. The gov.uk domain has strict security standards and monitors for threats and vulnerabilities.
For the Use of Social media: please read the IT and Email policy 10.1 – 10.5

1.4 Physical Security

Paper files, keys and devices are stored within the Parish Council office; sensitive information is kept in a locked safe/cabinet – the door to the office is also locked. Access to these files and the office computer and laptop are by password only and access granted to the Clerk and relief Clerk.

1.5 Data Backup

1.5.1 The parish council's data backup arrangements are managed by the IT support provider and consist of two independent layers to ensure recoverability in the event of hardware failure, accidental deletion, cyber-attack or disaster.

1.5.2 OneDrive (Microsoft Business Standard)

All council files are stored in Microsoft 365 OneDrive, which provides 1TB of cloud storage with built-in version control. This means that if a file is accidentally changed, overwritten or corrupted, previous versions can be recovered directly. OneDrive is the council's primary working file store and should be used for all parish council documents, records and correspondence.

1.5.3 Off-site cloud Backup (S3 Storage)

In addition to OneDrive, an independent cloud-to-cloud backup runs daily to a separate secure storage location. This provides a second, fully independent copy of council data that is not connected to the council's Microsoft 365 account. This ensure that even in the event of a ransomware attack or the compromise of the Microsft 365 account itself, a clean copy of council data can be restored.

1.5.4 Responsibilities

The IT support provider is responsible for configuring, monitoring and verifying that backups are running successfully, the typical schedule is every 3 months. Any backup failures will be investigated and resolved promptly. The Clerk is responsible for ensuring that all council files are saved to the OneDrive rather than solely on the local PC, so that they are captured by both backup systems. Backup integrity will be tested at least once per year by the IT support provider to confirm that data can be restored successfully. The council should not rely on files stored only on the local PC or on USB drives as a backup method.

1.6 Data Retention

For detailed guidance please read the Document Retention policy. Data retention periods should be followed as set out in the data processing map held by the Clerk and updated annually.

1.7 Erasure of Data

- When personal data is no longer required, or a data subject has exercised their right to erasure under GDPR Article 17, the data will be deleted promptly and securely. For electronic files stored on the council's PC, deletion will be carried out by removing the file and then emptying the Windows Recycle Bin. Files store in Microsoft 365 OneDrive will be deleted and then removed from the OneDrive recycle bin to ensure they are no longer retained in the cloud.
- Where data is particularly sensitive, or where the council needs to ensure that deleted data cannot be recovered by any means (for example, prior to the disposal of repurposing of a device) the Clerk will submit a request to the IT support provider, who will carry out the secure erasure using specialist software.
- Paper records containing personal data will be shredded before disposal.
- The Clerk is responsible for ensuring that erasure requests are actioned promptly and recorded appropriately.

1.8 IT Security and Storage

To enable robust IT security the parish council have in place:

- An IT Risk Review led by the IT Support Provider
- Annual Report to the Parish Council
- Professional antivirus and DNS website filtering
- OneDrive versioning plus a cloud backup for full recoverability
- Cyber Security Policy (included in this policy)
- Incident response Guide
- Staff Leaving Checklist
- IT Equipment Asset register

2. Cyber Security

2.1 What is cyber security?

A local council routinely holds and uses information about individuals in the performance of its statutory functions, powers and contractual obligations; consequently they are at risk from digital attacks, theft or unauthorised access. Cyber security is the practice of protecting systems, networks, programs and data from risk.

2.2 Passwords

All user accounts must be protected by strong, secure passwords. **For more detailed guidance please refer back to 1.2 in this policy and the IT and Email policy siblehedingham-pc.gov.uk/policies-and-procedures/**

- **Password and Authentication policy 5.1**
- **Access to passwords 6.1**
- **Password storage and management 6.2**
- **Password change requirements 6.3**
- **Password access control and logging 6.4**
- **Responsibility 6.5**

2.3 Malware

Malware is malicious software which is designed to disrupt, damage or gain unauthorised access to computer systems and devices. The parish council has updated its IT equipment and has professional antivirus and DNS website filtering – **please refer back to 1.8 – IT Security and storage.**

2.4 Data Backup

Please refer back to 1.5

2.5 Recognition

Councillors, staff and other authorised users must not assume every email they receive is genuine and will:

- Carefully check the senders address
- Be cautious of inks and attachments
- NEVER provide passwords r private information
- Beware of generic greetings i.e. Dear valued customer; if unsure they will check the company the email is supposedly from
- Check for spelling or grammatical errors

2.6 Reporting

Cyber incidents should be reported online ico.org.uk and also reported to www.reportfraud.police.uk
Councillors, staff and other authorised users will report phishing emails or texts to report@phshing.gov.uk or text 7726

Version 1

Adopted: 1 June 2026

Review: June 2027

Signed by the Chairman: ……

Date …….